MP 99B0000020R1SUPP2

MITRE PAPER

State of the Art in CyberSecurity Monitoring

A Supplement

September 2001

Leonard J. LaPadula

Sponsor: United States Air Force
Department: G021
Contract: F19628-99-C-0001
Project: 03017499-RC

Center for Integrated Intelligence Systems
Bedford, Massachusetts

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2001		**00-09-2001 to 00-09-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
State of the Art in CyberSecurity Monitoring. A Supplement	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **MITRE Corporation,202 Burlington Road,Bedford,MA,01730-1420**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**17**	

Preface

This paper is a supplement to my report on the state of the art in cybersecurity monitoring (CSMn) systems [1] and depends heavily on its companion paper, the CSMn compendium [2]. Both papers are revisions of the original 1999 publications.

In September 2000, I issued an update to the state of the art paper. [3] The update took a new look at the commercial marketplace, based on the then latest CSMn compendium published in August 2000, to discern any trends and identify new kinds of products. Some new research and development initiatives were identified. Finally, the update offered commentary on the relationship between the commercial sector and our military sponsors and what the state of affairs might augur.

The current supplement neither incrementally extends the referenced update nor replaces it. Rather, this supplement takes an independent look at the commercial products in the CSMn area and speculates on what the findings may mean to our military sponsors.

State of the Art in CyberSecurity Monitoring: A Supplement

One of the tenets of knowledge management these days suggests that telling a story transfers knowledge very effectively with most people. The reader will understand from that cue why the following imaginary press release leads off this supplement.

SupraSecure Systems[1] Unveils Security Management Strategy and Product Lineup

Delivers Central Enterprise Security Management SupraManager and Integration of SSS and TrendyWeb Security Products for Comprehensive Security Solution

Santa Mirari, California—July 2001— SupraSecure Systems (SSS) Corporation (Nasdaq: SSSC[2]), a leading provider of e-business infrastructure management solutions, today announced its strategy for centralized enterprise security management. SupraSecure Systems also announced today that it has combined and integrated security products from SupraSecure Systems and TrendyWeb to provide a comprehensive security management solution covering real-time security incident management and correlation, based on data generated by network-based intrusion monitoring, host-based intrusion detection, security policy management, vulnerability assessment, firewall security reporting, web server monitoring, user security administration, and file security administration components.

SupraSecure Systems' strategy is to provide an end-to-end security solution that enables organizations to effectively administer, assess, enforce, and protect all aspects of security in their enterprise. SupraSecure Systems today, via its SupraSecure Manager product, delivers an enterprise security management 'platform'. This platform provides a central, comprehensive view of the security of an enterprise's cyber resources. It enables correlation and management of security information across multiple operating systems, applications, anti-virus products, firewalls, network intrusion detection products, network devices, and vulnerability assessment products. Currently focused on Windows-centric enterprises, SupraSecure Manager will also offer support for heterogeneous operating systems including Windows NT, Windows 2000, Unix, and Linux.

This fictional press release took very little imagination to concoct since there are plenty of examples to use as models. Embedded within it are the kernels of ideas that this supplement will explore. Since early 2000, a discernible trend toward integration and

[1] The name of this company is purely fictional in this context; any similarity or equality with a real company's name is unintended.

[2] This symbol is purely fictional in this context; any similarity or equality with a real Nasdaq symbol is unintended.

expansion through development, acquisition, and partnering has developed. When a company perceives that its market position is threatened for lack of a particular category of tool or solution, it develops it, acquires it, "borrows" it through partnering, or gets out of the business[3]. The leaders in cybersecurity monitoring have expanded their view of what this technology encompasses, abandoning the approach of the early days of intrusion detection. In its initial growth spurt, back around 1996 and 1997, intrusion detection meant network packet monitoring using string pattern matching (signatures) and the race was on to incorporate and check more signatures than the competition could. Network-monitoring technology has matured well beyond this primitive approach. New techniques include protocol analysis and stateful inspection of sessions. Moreover, networking monitoring is now recognized as just one part of a cybersecurity monitoring system. As reflected in the fictional press release above, many vendors now market enterprise-security management solutions comprising

- Network monitoring
- System monitoring (host-based, workstations and servers)
- Vulnerability scanning (networks and hosts)
- Integrity monitoring (files, applications, operating system data)
- Security policy management (creating, monitoring, and maintaining)
- Firewall security reporting
- Web server monitoring

It would not be surprising to see this list expanding over the next several years. Two possibilities as additions to this list are decoys[4] and cages[5]. It is too early to tell whether these approaches will become popular: they are certainly interesting, but they have not yet proved their cost effectiveness in enterprise defense.

---

[3] Network Associates, Inc. announced in 2001 that it would no longer sell CyberCop Monitor, effectively withdrawing from the competition in network intrusion detection (it did not drop all of its other security solutions). Symantec acquired Axent in 2000. [4] Internet Security Systems announced on June 6, 2001 that it had completed acquisition of privately-held Network ICE Corporation. [press release at www.networkice.com]

[4] A decoy tool or system provides, simulates, or emulates a computer system or network appliance, providing a target for a cyber attacker, whether insider or outsider. The purpose of a decoy can be to draw an attacker away from valuable cyber resources, to study the methods used by cyber attackers in order to develop better defenses, or to identify an attacker and gather evidence that can be used to prosecute the attacker for illegal activity. Tools of this type collect data about the intrusive activity, provide alerts and reports, and collect evidence to be used in legal action.

[5] We discuss cages shortly.

There are apparently few commercially available decoys today. One of the earliest was CyberCop Sting by Network Associates, Inc, which began shipping in late 1999. Since then, to our knowledge, only one additional commercial decoy[6] has come on the market, ManTrap by Recourse Technologies, Inc. If decoys prove their value, we would expect to see their integration into the kind of comprehensive cybersecurity management we mentioned above. Similarly, if cages pan out, they would join the arsenal of tools for comprehensive enterprise defense. We have seen only two cages[7], SAFETNET by Pelican Security and the Surfin family of products by Finjan Software—SurfinGate and SurfinShield.

In the short history of cybersecurity monitoring, the cage is a recent development and an excellent example of how cybersecurity monitoring has diversified since the development of network packet monitors that use signatures. A cage tool or system protects a system from potentially damaging Internet (or intranet) code—that is, any "downloadable" (to the system) data that is potentially executable or that can contain or create an executable. A cage, as opposed to other types of tools, does this from inside the system it protects: it watches applications that have the potential to download Internet code and, in some way, constrains the actions of their downloads according to a predefined policy, which would typically be determined by the using organization. Thus, a cage can protect a system from mobile code.

Tools such as cages and the many other types mentioned above, even when operated independently of each other, contribute to enterprise security management. When their operations are coordinated through a central cybersecurity manager, they collectively provide an enhanced level of protection and detection and enable informed decision making. Usually a commercial cybersecurity manager coordinates tools of the same vendor that provides the manager. However, this is not always the case. Some vendors' managers accept inputs from other popular products such as firewalls. Examples of such products are

- CyberWolf by Mountain Wave, Inc.
- SAFEsuite Decisions 2.6 by Internet Security Systems (ISS)
- Security Manager by NetIQ
- SPECTRUM Security Manager by Aprisma Management Technologies
- Tivoli Secure Way Risk Manager by Tivoli Systems, Inc.

Three of these systems use the same approach to gathering information from other vendors' products. CyberWolf, for example, uses Software Device Experts that must be installed in a network appliance such as a firewall. The Device Expert filters and interprets

---

[6] We know of one other decoy, provided as GOTS by Defense Information Systems Agency, called Intrusion and Misuse Deterrence System (IMDS); see Compendium, reference [2], for a description.

[7] Note that there may well be others—it is difficult to know of all the commercial offerings in this area—but we think they are few in number compared to the number of network and host-based monitors, vulnerability scanners, and so on.

audit events as they are produced by the security component and forward relevant security information to the CyberWolf information manager. Tivoli Secure Way Risk Manager and SAFEsuite Decisions use a similar approach. We were not able to determine the approach used by NetIQ and SPECTRUM Security Manager in the time available for compiling this kind of information. [2]

For communications between their managers and their agents, these systems use various approaches. SAFEsuite decisions uses SAFELink, ISS' automated data collection and report distribution technology for multiple sources and destinations. Tivoli Secure Way Risk Manager uses Intrusion Detection Exchange Format (IDEF), a draft IETF specification. CyberWolf uses SSL. The methods of the other two products are not known at this time.

Some products use or can use SNMP traps for sending data and/or communicating among components. We know of the following:

- CyberWolf
- Dragon Intrusion Detection System
- ManHunt
- SAFETNET

However, the more typical use of SNMP traps is to send alerts to a network management system. This is almost universal among commercial products that provide any kind of alert of suspicious activity or policy violation. Also, the SNMP trap is almost never the only alert used: typically it is only one option of several including e-mail, pager, and on-screen alert.

In their 1997 report on intrusion detection, Hill and Aguirre observed that there is growing recognition that there would be high utility in integrating the output of different entities involved in network security, including routers, firewalls, proxies, and host-based and network-based IDSs. [4] Likely, they were thinking of heterogeneous entities, a mix of various vendors' products and government products and prototypes. In spite of several standards efforts that would enable it, that level of integration has not occurred. However, the lesser achievement—that of integrating products of the same vendor—appears finally to be happening. In our 1999 state of the art report, we identified a trend toward suites of products. [1] A suite of closely related products of a vendor enables the integration of outputs of those products. Then, in the 2000 update to the report, we observed that one would be hard-pressed to continue claiming that there was such a trend. [3] Now, about one year later, it appears that the number of suites being offered slowly but surely continues to increase as vendors find market advantage in providing comprehensive enterprise solutions, as we discussed earlier.

We also observed last year, in the update to the report, that commercial vendors and military researchers/developers work on different aspects of the cybersecurity management problem and that this had been the case for several years. Although this still appears to be

largely the case, we think there may be a potentially significant change fueled by the continuing increase in e-commerce. E-commerce depends on trust and reliability; at the same time, it is threatened by Internet-based hacker/crackers as well as malicious insiders. Vendors appear to be responding to the needs of business, the ranks of those providing security solutions being added to by those who formerly focused only on communications infrastructure or network management solutions. Not surprisingly, since large e-commerce companies have or use networks not unlike those of the Air Force, the security solutions being developed by industry are moving closer to providing the kind of capability the Air Force needs. As evidenced by the tables and pie charts in the appendix, enterprise security solutions have increased dramatically in number over the past two years and simple sensor tools now form a smaller percentage of the tools surveyed in 2001.

This Page Intentionally Left Blank

List of References

1. LaPadula, L. J., September 2000, *State of the Art in CyberSecurity Monitoring*, MP 99B0000020R1, approved for public distribution, The MITRE Corporation, Bedford, Massachusetts.

2. LaPadula, L. J., August 2001, *CyberSecurity Monitoring Tools and Projects: A Compendium of Commercial and Government Tools and Not-For-Profit Research Projects*, MP 99B0000018R3, The MITRE Corporation, Bedford, Massachusetts. This document is not currently in the public domain; its predecessor **(***CyberSecurity Monitoring Tools and Projects: A Compendium of Commercial and Government Tools and Government Research Projects*) is publicly available.

3. LaPadula, L. J., September 2000, *State of the Art in CyberSecurity Monitoring: An Update*, MP 99B0000020R1Supp1, approved for public distribution, The MITRE Corporation, Bedford, Massachusetts.

4. Hill, W. H., and S. J. Aguirre, September 1997, *Intrusion Detection Fly-Off: Implications for the United States Navy*, MITRE Technical Report 97W0000096, The MITRE Corporation, McLean, Virginia. This document is not in the public domain. However, it provided an important source of information on the state of the practice as described in Reference 1 above. Information from this reference that was not reported in Reference 1 was not relevant to Reference 1, its update, and this supplement.

This Page Intentionally Left Blank

Appendix

Summary of COTS CSMn Products

This information was compiled on August 4, 2001 from the CSMn Compendium [2]. Highlight colors are used as follows:

- Green: this entry in the table is the same as the entry appeared in the update document [3] of about two years ago[8]
- Yellow: updated information for an entry that was there two years ago
- Turquoise: new entry compared to two years ago
- Gray: the tool appeared in the table two years ago but is no longer available and has been deleted from the compendium compared to two years ago

Name of Tool	Type	Released	Vendor
AntiSniff, Version 1.0 (July, 1999)	Network Scanner	July 1999	LOpht
AutoSecure Access Control (for Windows NT or for UNIX)	System Monitor for Access Control	≤ 1998	PLATINUM
AutoSecure Policy Compliance Manager	Security Compliance Scanner	≤ 1998	PLATINUM
BlackICE Defender	System Monitor (Personal Firewall and IDS)	August 1999	Network ICE
BlackICE Agent (formerly BlackICE Pro)	System Monitor	May 10, 1999	Network ICE
BlackICE Sentry	Network Monitor	1999	Network ICE
Centrax 3.1	Network Monitor System Monitor Vulnerability Scanner	June 30, 2001	CybeSafe

[8] Note that the date shown for the referenced document does not agree with this statement. The reason is that the date of the document referenced is the date of the revision that was published to modify the terminology used in the report. The date of the original document is February 24, 1999. The table entries in the revision are the same as those in the original update of 1999.

Name of Tool	Type	Released	Vendor
Cisco Secure Intrusion Detection System (formerly NetRanger)	Network Monitor	≤ 1998	Cisco
Computer Misuse Detection System (CMDS™)	System Monitor	≤ 1997	ODS Networks
CyberCop Monitor	System Monitor	1999	Network Associates
CyberCop Scanner, Version 2.5	Vulnerability Scanner	≤ 1998	Network Associates
CyberCop Server	System Monitor	1999	Network Associates
CyberCop Sting	Decoy	late 1999	Network Associates
CyberWolf	Intrusion Detection and Reaction Director	2000	Mountain Wave, Inc.
Database Scanner 1.0	Vulnerability Scanner	≤ 1998	Internet Security Systems
Dragon Intrusion Detection System, Version 4.1	Intrusion Detection System	March 2, 2001	Enterasys—a Cabletron Company (formerly Network Security Wizards)
Enterprise Security Manager	Security Compliance Scanner	≤ 1998	Symantec Corporation (via merger with Axent, 12/18/2000)
eTrust™ Intrusion Detection (formerly SessionWall)	Network Monitor	February 9, 1999 (as SessionWall)	Computer Associates
eNTrax Security Suite	System Monitor Vulnerability Scanner	≤ 1998	Centrax
Expert™ 4.1	Network Mapper Vulnerability Scanner Risk Analyst	≤ 1998	Symantec
HackerShield	Vulnerability Scanner	≤ 1998	BindView
ICEcap Manager	Intrusion Detection and Reaction Director	1999	Network ICE

Name of Tool	Type	Released	Vendor
ICEcap Security Suite	Suite of Tools	≤ 2001	Network ICE
ID-Trak	Network Monitor	≤ 1998	AXENT (by acquisition of Internet Tools, Inc.)
Internet Scanner	Vulnerability Scanner	≤ 1998	Internet Security Systems
Intruder Alert	Host-based Intrusion Detection and Policy Management	≤ 1998	Symantec Corporation (via merger with Axent, 12/18/2000)
IP-Watcher	Network Monitor	≤ 1998	En Garde Systems
IRIS (INTOUCH Remote Interactive Supervisor)	Intrusion Detection and Reaction Support Tool	≤ 1998	Touch Technologies
Kane Security Analyst for Novell	Vulnerability Scanner	≤ 1998	ODS Networks
Kane Security Analyst for Windows NT	Vulnerability Scanner	≤ 1998	ODS Networks
Kane Security Monitor for Windows NT	Infraction Scanner	≤ 1998	ODS Networks
ManHunt	Network Monitor	September 2000	Recourse Technologies, Inc.
ManTrap	Decoy	September 2000	Recourse Technologies, Inc.
NetDetector	Network Monitor	≤ 2001	NIKSUN, Inc.
NetBoy Suite of Software	Suite of Monitors	≤ 1998	NDG Software
NetProwler	Network Monitor	≤ 1998	Symantec, AXENT Technologies, Inc.
NetRecon, Version 2.0	Vulnerability Scanner	≤ 1998	AXENT
NetSonar	Vulnerability Scanner	≤ 1998	Cisco
NFR Network Intrusion Detection (formerly Network Flight Recorder)	Network Monitor	1999	NFR Security, Inc. (formerly Network Flight Recorder, Inc.)

Name of Tool	Type	Released	Vendor
NFR Secure Log Repository	Monitoring Support Tool	Post-1999	NFR Security, Inc.
NOSadmin for Windows NT, Version 6.1	Vulnerability Scanner	June 1999	BindView
Peakflow DoS	Network Monitor for Denial-of-Service Attacks	≤ 2001	Arbor Networks, Inc.
POLYCENTER Security Compliance Manager	Security Compliance Tool	≤ 1997	Touch Technologies, Inc.
POLYCENTER Security Intrusion Detector for Digital UNIX, Version 1.2A	System Monitor	≤ 1997	COMPAQ, DIGITAL Products and Services
POLYCENTER Security Intrusion Detector for OpenVMS VAX and OpenVMS Alpha, Version 1.2a	System Monitor	≤ 1997	COMPAQ, DIGITAL Products and Services
POLYCENTER Security Reporting Facility (SRF)	Intrusion Detection and Reaction Director	≤ 1997	COMPAQ, DIGITAL Products and Services
Polycenter Security Intrusion Detector	System Monitor	≤ 1997	Touch Technologies, Inc.
Polycenter Security Console	Cybersecurity Management Director	≤ 1997	Touch Technologies, Inc.
PréCis 3.0	Audit Management Toolkit	≤ 1998	Litton PRC
ProxyStalker 1.0	System Monitor	≤ 1998	Network Associates, Inc., Trusted Information Systems Division
RealSecure™ 3.1	Integrated Network Monitor and System Monitor	1999	Internet Security Systems
Retina	Network Vulnerability Scanner	≤ 2001	eEye Digital Security

Name of Tool	Type	Released	Vendor
Retriever™ 1.5	Intrusion Detection and Reaction Director	1999	Symantec
SAFEsuite Decisions 2.6	Intrusion Detection and Reaction Director	≤ 1998	Internet Security Systems
SAFETNET	Cage	≤ 2000	Pelican Security
SAINT™	Network and Vulnerability Scanner	≤ 1998	World Wide Digital Security, Inc.
SecureNet Pro	Network Monitor	1997	MimeStar
Security Configuration Manager for Windows NT 4	Security Compliance Scanner	≤ 1998	Microsoft
Security Manager	Director	July 2001	NetIQ Corporation
SeNTry – Enterprise Event Manager	System Monitor	≤ 1998	Mission Critical Software
SFProtect - Enterprise Edition	Vulnerability Scanner Security Compliance Scanner	August 1999	Hewlett Packard
SilentRunner	Discovery, Visualization, and Analysis Tool	≤ 1999	Raytheon; reseller and product suppor: Internet Security Systems
SMART Watch	System Monitor (System Integrity Checker)	June 8, 1998	WetStone Technologies, Inc.
SPECTRUM Security Manager	Analyzer (Integrated Cybersecurity Monitor)	2000	Aprisma Management Technologies
Stake Out™ I.D.	Network Monitor	≤ 1998	Harris Communications
Stalker, Version 2.1	System Monitor	≤ 1998	Network Associates, Inc., Trusted Information Systems Division

Name of Tool	Type	Released	Vendor
System Scanner 4.2	Vulnerability Scanner Infraction Scanner	≤ 1998	Internet Security Systems
Tivoli® SecureWay® Risk Manager	Intrusion Detector and Reaction Director	≤ 2001	Tivoli Systems, Inc.
Tripwire for Servers	Integrity Monitor	≤ 2001	Tripwire, Inc.
Tripwire Manager	Director	≤ 2001	Tripwire, Inc.
T-sight™	Analyzer and Responder (Intrusion Investigation and Response Tool)	2000	En Garde Systems, Inc.
VigilEnt Security Manager	Security Compliance Manager	≤ 2001	PentaSafe Security Technologies, Inc.

Table A-1. Count of Tools by Architectural Type

Type	1999 Count	2001 Count
Sensor (standalone)	28	38
Sensors-Director (single type sensor)	13	24
Enterprise Security Manager (Sensors-Director, various type sensors)	1	6

The pie charts that follow graphically display the counts in the table above.